新疆维吾尔自治区第二届职业技能大赛

网络安全项目

技术工作文件

大赛组委会

2024 年 9 月

目　录

一、技术描述

（一）项目概要

网络安全项目竞赛需要选手保护企业的信息系统，防止黑客访问和窃取企业的敏感数据。网络安全项目竞赛选手通过配置防火墙、入侵检测系统、服务器等网络安全设备，制定网站安全解决方案来保护企业的系统不被入侵。同时，还需要维护并实施企业的网络安全监控系统策略，调查发生在企业内部的网络安全事件。选手需要对企业的信息系统进行安全渗透测试，提前发现可能被黑客利用的漏洞并及时对漏洞进行修补和安全加固。

网络安全项目竞赛还需要选手能够保障虚拟化基础设施的安全,开展相关的信息安全活动，通过代码审计、用户流量分析、渗透测试等技术手段来保障企业的关键数据不被盗取、篡改和破坏。

选手需要进行数字调查取证，收集、保存、处理、分析和提供与计算机相关的证据，通过技术手段协助执法机构侦破网络犯罪和防范网络欺诈。

在一个快速发展的行业，选手必须比潜在的网络攻击者领先一步。选手必须掌握攻击者用来渗透相关信息系统的最新方法，以及最新的安全技术，来帮助组织确保系统的安全性以应对这些威胁。

选手应同时具备表达、书写、沟通、协调等能力，具有较高综合素质。

（二）基本知识与能力要求

选手基本知识与能力要求表：

相关要求		权重比例(%)
1	工作组织和管理	
基本知识	选手需要了解和理解： —健康与安全相关的法规、义务、规定和文档 —必须使用个人防护用品的场合，如：静电防护 —在处理客户设备和信息时的完整性和安全性 —废物回收、安全处置的重要性 —计划、调度和优先处置的方法	5

	—在所有的工作过程中,准确、检查和注意细节的重要性 —系统性开展工作的重要性	
工作能力	选手应具备的能力： —遵守健康和安全标准、规则和规章制度 —保持安全的工作环境 —识别并使用适当的个人静电防护设备 —安全、妥善地选择、使用、清洁、维护和储存工具和设备 —规划工作区域，最大化工作效率，并维持日常整洁的相关规定 —有效地工作，并定期检查进度和结果 —保持与职业岗位要求一致的技能水平 —采取全面有效的研究方法，确保知识不断更新 —主动尝试新方法、新系统并愿意接受变革	
2	**沟通和人际交往**	10
基本知识	选手需要了解和理解： —倾听作为有效沟通一部分的重要性 —作为同事的角色、要求和最有效的沟通方式 —与同事和管理人员建立和保持创造性的工作关系的重要性 —有效的团队合作技巧 —消除误会和化解冲突的技巧 —管理紧张和愤怒情绪 —网络安全调查的过程需要有完整的文档记录	
工作能力	选手应具备的能力： —加强倾听和提问技巧，加深对复杂情况的理解 —保持有效的队友之间的口头和书面沟通 —识别和适应队友变化的需求 —为发展强大而有高效率的团队作出积极贡献	

	—与队友分享知识和专业技能，发展出相互支持的学习文化 —管理好紧张/愤怒等情绪，遇到问题能有解决的信心 —调查过程中准确地记录步骤和发现结果 —确保所有安全和信息系统操作方面的政策和工作流程都被严格遵守	
3	**安全系统的设计和建设**	10
基本知识	选手需要了解和理解： —IT 风险管理的标准，策略，需求，和工作流程 —网络安全防护和脆弱性的检测工具及其功能 —操作系统 —网络系统 —计算机编程概念，包括计算机语言、编程、测试、调试和计算机文件种类 —软件开发的网络安全、隐私保护的原则和方法	
工作能力	选手应具备的能力： —在设计和记录总体程序测试和评估过程时，应将网络安全和隐私原则应用于组织要求（与保密性、完整性、可用性、可控性、不可否认性相关） —独立进行综合测试，包括管理、运行和技术安全控制、信息系统内部或者源自信息系统的增强控制功能等，判断、决定整体控制效果 —开发、使用网络安全评估系统,以评估相关系统符合规范和要求 —确保合并 IT 系统元素的安全性和系统的互操作性 —修改现有的计算机应用程序、软件或专门应用程序 —分析新的或者现有计算机应用程序、软件的安全状况，提供准确可靠的分析报告 —开发和维护业务、系统和信息流程以支持企业任务需求	

	—开发描述基线和信息系统体系结构的技术规则和要求 —确保利益相关各方安全需求，保护企业运营和商业流程在企业架构的各个方面得到正常处理，包括参考模型、部分和解决方案架构、确保系统支持企业的运营和商业流程 —对系统工程和软件系统进行安全研究，开发相应的安全功能，并将其部署系统中 —开展研究（包括渗透测试）来评估网络空间系统中潜在的脆弱性 —咨询相关人员，评估功能需求，并将功能需求转换为技术解决方案 —计划、准备和实施系统测试 —根据技术规范和要求，进行分析、评估并报告结果 —设计、开发、测试和评估信息系统的安全情况，涵盖系统开发生命周期	
4	**操作、维护、监督和管理**	15
基本知识	选手需要了解和理解： —查询语言，如结构化查询语言、数据库系统等 —网络协议，如 TCP/IP、动态主机配置、DNS 和目录服务等 —防火墙概念和功能（如单点身份验证、审核、策略执行，恶意内容的邮件扫描，PCI 和 PII，遵从性数据匿名化，数据丢失保护 扫描，加速加密操作，SSL 安全，REST、JSON 处理等） —网络安全体系结构的概念，包括拓扑、协议、组件和原则 —系统管理、网络和操作系统加固技术 —组织信息技术用户安全策略（如帐户创建、密码规则、访问控制 等） —信息技术安全原则和方法 —身份验证、授权和访问控制方法	

	—网络安全、漏洞和隐私原则	
工作能力	选手应具备的能力： —安装、配置、测试、操作、维护、和管理网络体系架构 —管理好分享和传输所有数据的软件 —安装、配置、调试和维护服务器（硬件和软件），确保信息保密性、完整性和可用性 —系统密码、账户的创建和管理，并实施相应的访问控制策略 —分析机构当前的计算机系统，设计信息系统解决方案，以帮助机构更安全、高效和有效地运行 —开发监视和测量风险、合规性和保证工作的方法 —对信息系统、基础设施网络进行审计，以提供持续优化、网络安全和解决问题的支持	
5	**安全系统的保护和防卫**	15
基本知识	选手需要了解和理解： —文件系统 —系统文件（如日志文件、注册表文件、配置文件等）包含相关信息以及在何处查找这些系统文件 —网络安全体系结构的概念，包括拓扑、协议、组件和原则(如纵深防御的应用) —行业标准和组织性接受的分析原则、方法和工具来识别漏洞 —威胁调查、报告，调查工具和法律、条例 —事件类别、响应和处理方法	
	—网络防御和漏洞评估工具及其功能 —对于已知的安全风险的应对措施设计 —身份验证、授权和访问方法（如基于角色的访问控制、强制访问控制和任意访问控制等)	
工作能力	选手应具备的能力：	

	—使用防护措施和不同渠道收集的信息，以识别、分析和报告发生的或可能发生的网络事件，以保护信息、信息系统和网络免于威胁 —测试、实施、部署、维护、检查、管理硬件基础架构和软件，按要求有效管理的计算机网络防护服务提供商的网络和资源 —监视网络，及时修订未授权的活动 —在所属的领域对危机或者紧急状态做出有效响应，在自己的专业领域中降低直接的和潜在的威胁 —使用缓解措施、准备措施，按照要求做出响应和实施恢复步骤，以最大化存活率，保存财产和信息的安全 —调查和分析所有的相关响应活动 —对威胁和漏洞进行评估 —确定与可接受的配置、企业或本地策略的偏差 —评估风险水平，制定或建议在业务和非运营情况下采取适当的缓解措施 —根据记录好的企业工作流程开展安全事件的灾备和恢复	
6	**操作和管理**	
基本知识	选手需要了解和理解： —网络威胁行为者，他们的资本和他们的方法 —用于检测各种可利用的活动的方法和技术 —网络情报和信息收集能力 —网络威胁和漏洞 —网络安全基础知识（如加密、防火墙、认证、诱捕系统、外围保护等） —漏洞信息传播源（如警报、通知、勘误表和公告等） —哪些系统文件（如日志文件、注册表文件、配置文件）包含相关信息以及在何处查找这些系统文件 —开发工具的结构、方法和策略（如嗅探、记录键盘等）和技术（如获取后门访问、收集机密数据、对网络中的其他系	20

	统进行漏洞分析 等) —预测、模拟威胁能力和行动的内部策略 —内部和外部合作伙伴的网络操作能力和工具使用能力 —目标开发（如概念、角色、责任、产品等） —系统开发过程遗留物和司法鉴定应用案例 —应用于现有已安装系统和软件的新兴网络攻击和网络威胁 —为防止自然灾害进行灾备的重要性	
工作能力	选手应具备的能力： —识别和评估网络安全罪犯或外国情报机构的能力和活动 —提供调查结果，来帮助法律程序和反间谍调查（或反间谍活动）的启动，或支持法律程序和反间谍调查（或反间谍活动）的执行 —分析搜集到的信息，找到系统弱点和潜在可被利用的环节 —分析来自情报界的不同渠道、不同学科和不同机构的威胁信息 —根据背景情况，同步和放置情报信息，找出可能的影响 —应用来自一个或多个不同地区、国家、非政府机构和技术领域的最新知识 —应用语言、文化和专业技术知识，进行信息收集、分析和其他网络安全活动 —识别、保存和使用系统开发过程遗留物并用于分析 —数据丢失时，成功执行数据和系统恢复	
7	**情报收集与操作**	10
基本知识	选手需要了解和理解： —收集策略、技术和工具 —网络情报获取和信息收集能力 —信息需求和收集要求在扩展的企业中被翻译、跟踪和优先处理	

	—需要与网络运营规划相关的智能规划产品 —网络运营规划计划、战略和资源 —网络操作策略、资源和工具 —网络操作概念、术语、词汇（如环境准备、网络攻击、网络防御 等)、原则、能力、限制和效果	
工作能力	选手应具备的能力： —使用适当的策略，创建的优先级别，通过收集管理过程进行数据收集 —支持收集网络犯罪或者外国情报机构证据活动，减轻可能的实时威胁，应对间谍和内部威胁、外国破坏行动、国际恐怖组织活动，或者为情报活动提供支持	
8	**调查和电子取证**	15
基本知识	选手需要了解和理解： —威胁调查、报告、调查工具和法律 —恶意软件分析的概念和方法 —收集、打包、传输和储存电子证据的过程，同时维持监管链 —持久性数据的类型和集合 —数字取证数据处理的概念和实践 —数字取证数据的类型和识别方法 —操作系统结构和操作对于取证的意义 —网络安全漏洞的具体操作性影响	
工作能力	选手应具备的能力： —收集、处理、保留、分析和展示计算机相关的证据，网络弱点的减轻措施（如犯罪、欺诈、反情报等），以支持司法部门的调查。	
合计		100

二、试题与评判标准

（一）试题（样题）

试题试题以第 46 届世界技能大赛、2022 世赛特别赛和中华人民共和国第二届职业技能大赛网络安全项目技术文件为依据，并结合世赛发展趋势和国内行业实际来组织命制。考核试题只考核技能部分，相关理论知识包含在技能考核中，所有试题评分标准采用测量评分。试题分为 3 个独立的模块，考核范围参见下表。

考核模块内容分值表

序号	模块名称	分值
1	模块 A 企业基础设施安全	35
2	模块 B 网络安全事件响应、数字取证调查和应用安全	35
3	模块 C 夺旗挑战（CTF）	30

本次竞赛（各模块）难度应不高于在世界技能标准规范（WSOS） 8 个方面规定的网络安全功能，难度等级应等价于以下认证水平：

1.Certified Information Security Professional：注册信息安全专业人员（CISP）

2.Certification Information System Security Professional：信息系统安全专业认证（CISSP）

3.Cisco Certified Network Professional(CCNP)：思科认证网络专业人员

4.Microsoft Certified Solutions Expert(MCSE)：微软认证解决方案专家

5.高级 Linux 认证 LPIC-2 或等效技能

（二）比赛时间及试题具体内容

1.比赛时间安排

本项目比赛总时间为 10 个小时，分为 3 个模块，共需 2 天完成，各模块的时间分配如下表所示：

日程	模块编号	模块名称	时间分配
C1	A	企业基础设施安全	3 小时
C2	B	网络安全事件响应、数字取证调查和应用安全	3.5 小时
	C	夺旗挑战（CTF）	3.5 小时
总计			10 小时

2.试题简述

（1）模块 A

模块 A 的任务是根据实际信息安全服务的工作内容进行设计，以典型组织机构的信息系统网络架构为基础，已实现网络的基本互通，但不满足网络安全行业最佳实践。选手需要使用各种网络安全技术对已有的网络和服务进行配置和加固。模块 A 的任务场景中的一些安全配置比较明确，但另外一些安全配置则为不同的实现选项预留了选择空间，选手需根据行业最佳实践（在安全性、高可用性和可扩展性方面）选择合理的安全方案，并尽最大努力实现安全配置。选手应该熟悉主流网络及安全设备、Windows、Linux 等主流操作系统和相应的服务组件的安全配置及加固技术。

（2）模块 B

模块 B 包含网络安全事件响应、数字取证调查和应用安全。该模块需要选手根据企业所发现的安全事件，展开网络安全事件的调查、分析和取证工作，收集、保存、处理、分析和提取计算机与网络相关的证据，分析黑客的入侵行为和代码弱点。模块 B 主要考察选手网络安全事件应急处置能力、网络安全事件取证分析能力、应用程序的逆向分析和代码审计能力以及网络安全风险评估防控能力。

（3）模块 C

模块 C 为夺旗挑战赛（CTF），选手需要在一个指定的网络安全攻防靶场中模拟攻击方，综合运用所掌握的网络安全技能，开展网络渗透测试。在比赛期间，参赛队伍可以利用给定的网络安全渗透测试工具对所提供的网络安全攻防靶场环境进行综合分析、挖掘和渗透。靶场环境中预设了若干 Flag，每个 Flag 有预设的分值，选手要尽可能多的获取 Flag 值。

（三）评判标准

1.分数权重

本项目评分为测量评分，各模块分数权重如下表：

模块编号	模块名称	分数权重
A	企业基础设施安全	35%
B	网络安全事件响应、数字取证调查和应用安全	35%
C	夺旗挑战（CTF）	30%
总计		100%

本次竞赛评分表参考世界技能大赛和中华人民共和国第二届职业技能大赛网络安全项目的评分标准制作。评分标准样例表如下：

子项 ID	子项名称或描述	评分细则	正确分值	得分值

样例：登录及密码策略配置评分表

子项 ID	子项名称或描述	评分细则	正确分值	得分值
A1	账户密码策略配置	最小密码长度不得少于 10 个字符(Windows)	0.2	0.2
		最小密码长度不得少于 10 个字符(Linux)	0.1	0.1
		所有密码必须作为可逆密文存储在配置中（网络设备）	0.3	0

2.评判方法

裁判长组织裁判员按照“公平、公正、公开”的原则开展执裁工作。本项目 A 模块评分为测量评分，评判过程按照评分标准进行独立客观评分，每题超过半数打分裁

判打分成绩一致方为有效得分，为确保评分过程的公平性和公正性，所有选手答题文件加密后交给评分裁判评分；B 模块和 C 模块采取计算机智能评分方式。

裁判员完成所有参赛选手评分后，对本人参与的评判结果进行核对确认，裁判长对总成绩进行复核。如在执裁和评分过程中出现争议的，由裁判长组织全体裁判员讨论，以获得半数以上票数为裁定结果。

3.成绩并列

各参赛队最终总成绩为 A、B、C 三个模块成绩之和，当出现选手总成绩并列时，本赛项按照 C、B、A 模块顺序进行得分排序。首先以 C 模块得分排序，如果 C 模块得分相同，再以 B 模块得分进行排序，以此类推。

（四）公布方式

本项目 A 模块试题和评分标准公开，B、C 模块为保密模块，试题和评分标准保密。赛前 10 天向选手公布 A 模块样题及评分标准，B、C 模块命题思路和样题。

赛前 2 天裁判长结合赛场设备、材料状况，按照本项目试题调整的工作流程和方法，组织裁判员对 A 模块样题进行不超过 30%的修改、调整，并进行试题验证、制作评分标准。试题经裁判长审核确认后即为本次竞赛的最终试题。按照本项目世赛规范，最终 A 模块试题确定后给予裁判组内部公开，但不对外公开发布。本项目 B、C 模块试题比赛现场裁判长向选手公布。

三、竞赛细则

（一）抽签方式、比赛轮次

比赛轮次为一轮次，每场比赛采用抽签的方式确定工位。比赛前选手经过一轮次抽签，确定本场比赛工位号。

（二）防止并列的措施

各参赛队最终总成绩为 A、B、C 三个模块成绩之和，当出现选手总成绩并列时，本赛项按照 C、B、A 模块顺序进行得分排序。首先以 C 模块得分排序，如果 C 模块得分相同，再以 B 模块得分进行排序，以此类推。

（三）预期分组与分工方案

裁判组下设若干裁判小组，每个裁判员只能参加一个小组的执裁工作，各小组独立负责各自任务部分的竞赛过程的完整工作，相互之间不相重合。

本项目的裁判员必须严格按照执裁流程和裁判员岗位内容完成执裁工作，包括相关技术性文件的学习。裁判员在执裁过程中需要全程参加整个执裁和评分过程，包括赛前的技术讨论，选手进场的抽签，执裁过程中的监督与问题处理，评分，竞赛成绩的汇总、确认等。

（四）裁判员在执裁中的纪律和要求

1．裁判员在执裁中必须服从裁判长和竞赛组委会的管理，遵守裁判员的职业道德，文明执裁。

2．裁判员应坚守岗位，不迟到早退。无特殊情况不得在竞赛期间请假。在执裁过程中需要暂时离开的，必须向裁判长申请，得到许可后方可离开。

3．裁判员在执裁过程中不得故意妨碍、影响任何选手的操作。

4．裁判员执裁过程中不能与自己的选手进行任何交流，不能进入到本队选手工位，裁判员在处理竞赛过程中选手提问的时候，不得单独行动，需要两名以上裁判员一起进行处理（裁判员不得介入自己选手问题的处理）。

5．裁判员在执裁过程中必须遵守“公正、公开、公平”的竞赛原则，严格按照竞赛技术规则和评分标准进行执裁。裁判员必须按照评分标准的要求操作步骤进行操作，不得对选手的配置做任何修改和调整。

6．裁判员应根据技术文件要求做好试题保密工作。在正式公布成绩和名次前，裁判员不得对外透露选手的成绩和排名情况。

7．裁判员在讨论试题和执裁期间，手机等电子产品需统一管理。

8．裁判员在参加赛前赛题讨论会时要严格遵守会议纪律，会议期间不能携带手机、相机等电子产品对会场进行录音和拍照，不能私自带走比赛讨论资料。

（五）赛场规则

1.所有竞赛软件工具由赛场提供；

2.各参赛队要发挥良好道德风尚，听从指挥，服从裁判员，不弄虚作假。如发生弄虚作假者，取消参赛资格，成绩无效；

3.正式比赛期间，各参赛队领队和其他人员可到赛场观摩，但需要按照赛场的安全管理要求在指定地点观摩，并服从现场工作人员的指挥和管理；

4.各参赛队应加强对参赛人员的管理，督促参赛选手要执行竞赛的各项规定，做好赛前准备工作；

5.对项目内处理结果有异议的，在选手成绩最终确认锁定前，由领队向组委会监督仲裁组出具署名的书面反映材料并举证；

6.竞赛期间参赛选手不得携带手机等移动通信或上网设备，不得携带移动存储设备、资料等物品；

7.因设备自身故障导致选手中断竞赛，无法继续比赛的，经确认后由裁判长视具体情况做出裁决；

8.选手在竞赛过程中不得擅自离开赛场，如有特殊情况，需经裁判员同意后作特殊处理，但因此引起的休息、饮水或去洗手间等所消耗的时间计算在竞赛操作时间内；

9.参赛选手若提前结束竞赛，应向裁判员举手示意，竞赛终止时间由裁判员记录，参赛选手签字确认，结束竞赛后不得再进行任何操作；

10.各赛场除现场裁判员、赛场配备的工作人员以外，其他人员未经裁判组允许不得进入赛场；

11.比赛期间，选手及当值裁判员在规定时间内可进入竞赛区域的选手操作区，当值裁判员应在指定岗位执裁，裁判长可进入全部竞赛区域。场地经理及相关赛务保障人员应在非操作区待命并按裁判长要求第一时间进入操作区处理问题；

12.如在执裁和评分过程中出现争议的，由裁判长组织全体裁判员讨论，以获得半数以上票数为裁定结果。

（六）违规处理

1.裁判员参加试题修改讨论会时要严格遵守会议纪律要求，如违反会议纪律，导致比赛资料外泄，除取消本参赛队比赛资格，还要承担相应的法律后果。

2.选手不得携带任何资料进入竞赛区，在比赛过程中发现选手有抄袭行为的，取消本次比赛资格。

3.选手扰乱赛场，干扰裁判员工作，视情节扣5～10分，情况严重者取消比赛资格。

4.裁判员严格遵守比赛规则，比赛期间不能与自己的选手有任何的单独接触行为，如果发现裁判员为自己选手提供有违比赛公平的信息，一经查实取消该参赛队的比赛资格。

5.裁判员评分期间，裁判员不能单独接触自己选手的电脑和环境，如发现裁判员有违反比赛规则的行为，选手本次比赛的成绩作废。

6.裁判员应严格执行评分规则，如裁判员存在恶意评分行为，将取消该裁判员执裁资格。

7.裁判人员具有以下违规行为之一记 1 次严重警告：

（1）拒不服从大赛组委会、执委会或裁判长技术工作安排，经提醒无效；

（2）擅自或伙同他人修改竞赛试题，更改工位（设施设备、工具、材料等）设置或窃取、擅自更改、编造或者虚报评判数据、信息；

（3）同其他裁判人员串通，对选手进行恶意评分；

（4）利用职权为选手作弊提供条件；

（5）默许、纵容或伙同他人集体作弊；

（6）利用职务便利从事任何影响公平公正的咨询、培训、竞赛、推销、赞助，特别是竞赛设施设备品牌确定等活动，经提醒无效；

（7）发现异常情况，拖延、瞒报，造成恶劣影响；

（8）行贿或受贿，以权谋私；

（9）擅自传播、扩散未经核查证实的言论、信息；

（10）未按规定在参赛选手评判结果上签字，经提醒无效；

（11）未按要求参加赛前培训、拒不签署《竞赛行为规范》；

（12）其他同等程度的违规行为。

8.选手具有以下违规行为之一计 0 分：

（1）在需要选手信息保密的项目或模块中，故意显示可使裁判人员辨识的本参赛团特征或选手本人特征信息；

（2）携带禁止携带的物品等作弊行为；

（3）其他同等程度的违规行为。

（七）赛程安排

网络安全项目竞赛正式时间为期 2 天，其中 C-1 为选手熟悉场地，C1 为 A 模块比赛，C2 为 B 模块、C 模块比赛。赛事日程安排如下所示：

1.整体安排

时间	主要事项
C-2	裁判员赛前培训、裁判员执裁分组、裁判员试题讨论和赛题确定
C-1	选手熟悉竞赛设备和竞赛环境
C1	A 模块比赛和评分
C2	B 模块比赛和评分
	C 模块比赛和评分，得分汇总统计
	技术点评会

2.具体安排

C-2 时间安排表

时间	事项	参与人员	负责人
10:30-13:30	裁判员赛前培训、裁判员执裁分组、裁判员试题讨论和赛题确定	裁判长 裁判长助理 全体裁判员	裁判长

C-1 时间安排表

时间	事项	参与人员	负责人
16:00-17:00	选手熟悉场地、竞赛设备和竞赛环境	裁判长 裁判长助理 全体裁判员 场地经理 选手	裁判长
17:00-18:00	设备设施恢复	裁判长 裁判长助理 全体裁判员 场地经理	场地经理
18:00-18:30	封场	裁判长 裁判长助理 场地经理	裁判长

C1 时间安排表

时间	事项	参与人员	负责人
13:00	工作人员、裁判员报到	工作人员 裁判长 裁判长助理 全体裁判员	场地经理
13:00-13:20	赛前裁判会议	裁判长 裁判长助理 全体裁判员	裁判长
13:20-14:00	选手检录、抽签、裁判长赛前介绍	裁判长 裁判长助理 全体裁判员 选手	裁判长
14:00-17:00	A 模块比赛	裁判长 裁判长助理 全体裁判员 选手	裁判长
17:00-17:30	A 模块收卷	裁判长 裁判长助理 全体裁判员 选手	裁判长
17:30-19:30	A 模块评分	裁判长 全体裁判员	裁判长
19:30-20:00	A 模块成绩确认	裁判长 裁判长助理 全体裁判员 录分员	裁判长
20:00	封场	场地经理	场地经理

C2 时间安排表

时间	事项	参与人员	负责人
9:20	工作人员、裁判员报到	工作人员 裁判长 裁判长助理 全体裁判员	场地经理
9:20-9:40	赛前裁判会议	裁判长 裁判长助理 全体裁判员	裁判长
9:40-10:00	选手检录、抽签、裁判长赛前介绍	裁判长 裁判长助理 全体裁判员 选手	裁判长
10:00-13:30	B 模块比赛	裁判长 裁判长助理 全体裁判员 选手	裁判长
13:30-13:50	B 模块成绩确认	裁判长 裁判长助理 全体裁判员 选手 录分员	裁判长
13:50	封场、休息	裁判长 裁判长助理 全体裁判员 选手 场地经理	裁判长 场地经理
14:50-15:00	选手入场、裁判长赛前介绍	裁判长 裁判长助理	裁判长

		全体裁判员 选手	
15:00-18:30	C 模块比赛	裁判长 裁判长助理 全体裁判员 选手	裁判长
18:30-18:50	C 模块成绩确认	裁判长 裁判长助理 全体裁判员 录分员	裁判长
18:50-20:30	分数汇总统计	裁判长 裁判长助理 场地经理 全体裁判员	裁判长
20:30-21:00	项目技术点评	选手 裁判长 裁判长助理	裁判长

注：竞赛时间安排具体以现场通知为准。

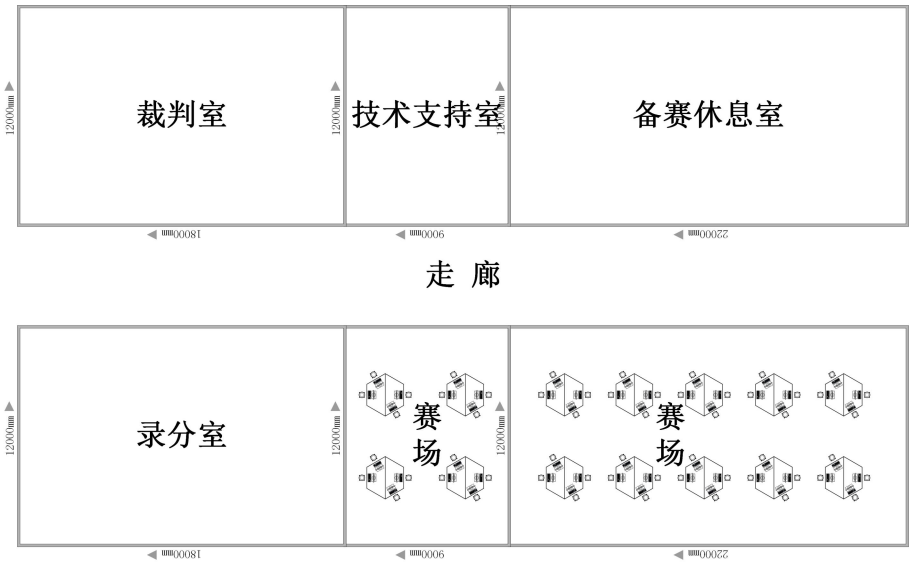
四、竞赛场地、设施设备等安排

（一）赛场规格要求

竞赛场地位于喀什技师学院 5 号楼 3 楼，本项目场地总体面积 1300 平方米（长 49 米、宽 27 米），赛场的布置充分利用现有建筑物的布局，竞赛室最大支持工位数量 28 个，每个工位的面积 8-12 平方米，同时设置有备赛休息室、技术支持室、裁判室、录分室、赛场等工作区域。3 张梯形桌组成 1 个工位，工位之间采用隔断隔离，每工位配置两台 PC，PC 与机柜通过网线连接。

（二）场地布局图

网络安全项目场地布局图如下：



注：本场地布局图仅供参考，具体以实际竞赛场地为准。

（三）基础设施清单

（1）该项目无需选手自带工具、材料，禁止选手携带任何工具、材料进入赛场，赛场配发的各类工具、材料，选手一律不得带出赛场。

（2）竞赛场地。竞赛场地配备符合竞赛要求，竞赛现场设置竞赛区、裁判区、服务区、技术支持区。现场保证良好的采光、照明和良好通风；提供稳定的水、电和供电应急设备，提供足够的干粉灭火器材。同时提供所有指导教师休息室 1 间。

（3）竞赛设备。竞赛设备由主办方负责提供和保障，竞赛区按照参赛队数量准备竞赛所需的软硬件平台，为参赛队提供标准竞赛设备。

（4）竞赛工位。工位间距和场地空间必须符合竞赛要求，竞赛现场各个工作区配备单相 220V/3A 以上交流电源。每个竞赛工位上标明编号并用隔离带隔离，确保参赛队之间互不干扰，每个竞赛工位配备 2 把工作椅（凳）。

（5）技术支持区为技术支持人员的工作场地，为参赛选手竞赛提供网络环境部署和网络安全防范。

（四）竞赛设备清单（面向参赛选手）

1、硬件设备

序号	名称	品牌/型号/技术参数	单位	数量
1	竞赛平台	网络空间安全竞赛平台（含服务器）	套	1
2	电脑	台式电脑：I7 或 I5/16G 内存/1T 硬盘/千兆网卡/硬盘保护卡/23.8 寸显示器/预装 win10/office	台	56

2、软件清单

序号	软件名称	版本
1	VMwareWorkstation	16.X
2	Windows Server 2019	Datacenter
3	Windows 10 x64	Enterprise LTSC
4	Linux(Ubuntu)	20.04.x LTS
5	zenmap	7.x
6	splunk	9.x
7	Splunk forwarder	9.x
8	burpsuit	2.x
9	QR_Research	1.1.2.x
10	tweakpng-src	1.4.x
11	Apache	2.4.x
12	ModSecurity	2.9.x
13	Snort	2.x
14	vsftpd	3.x
15	Wireshark	3.4.x
16	openssl	1.x
17	Kali	Version2021.3
18	IDA free	7.x

序号	软件名称	版本
19	MariaDB	10.x
20	OllyDbg	Version1.10
21	Volatility	Version2.x
22	Autopsy	Version4.x
23	x64dbg	snapshot_2023-03-04_02-26
24	Jadx-gui	1.4.x
25	HxD Hex Editor	Version 2.x
26	StegSolve	1.4
27	audacity	3.1.0
28	pwndbg(GDB 插件)	2021.06.22
29	sagemath	9.1
30	Pwntools(python)	4.6.x
31	pyCryptodome(python)	3.14.x
32	Pillow (python)	8.1.2
33	vscode	X64
34	Word	Office 2019
35	Frp	0.38.0
36	Neo-reGeorg	v3.7.0
37	Putty	0.68
38	ultraVNC	1.4.x
39	CaptfEncoder	2.1.0
40	Cutter	2.x
41	CyberChef	v9.55.0
42	pefile(python)	v2023.2.7
43	cygwin	2.925
44	UEFITool	A66
45	Radare2	5.8.6
46	frida-server	16.0.x

序号	软件名称	版本
47	frida-tools	12.0.x
48	Android Studio	2022.2.1
49	Android Virtual Device	API33
50	Snipaste	2.4.-86
51	vnc	4.6.3
52	firefox	en-48
53	Google Chrome	v127.0.6533.120
54	Cisco 防火墙镜像	ASA 9.19
55	Cisco 交换机镜像	Cisco Catalyst 2900 Series
56	Cisco 路由器镜像	Cisco 3900 Series

五、安全、健康要求

（一）选手安全防护要求

1.参赛选手应严格遵守设备安全操作规程。

2.参赛选手停止操作时，应保证设备的正常运行，比赛结束后，所有设备保持运行状态，不要拆、动硬件连接，确保设备正常运行和正常评分。

3.参赛选手应遵从安全规范操作。

4.参赛选手应保证设备和信息完整及安全。

（二）选手禁止携带物品

本次比赛赛场提供选手比赛所需的设备，选手除禁止携带任何带有存储功能的电子产品进入赛场外，还需禁止携带如下物品：

1.任何储存液体、气体的压力容器。

2.任何有腐蚀性、放射性的化学物品。

3.任何易燃、易爆物品。

4.任何有毒、有害物品。

5.任何没有生产厂商或达不到国家安全标准的工具及设备。

6.任何可能危及安全问题的物品。

7.任何影响竞赛公平性的物品。

（三）赛事安全要求

1.承办单位应设置专门的安全卫生应急保障部，负责竞赛期间的健康和安全事务。包括检查竞赛场地、与会人员居住地、车辆交通及其周围环境的安全防卫；制定紧急应对方案；监督与会人员食品安全与卫生；分析和处理安全突发事件等工作。

2.赛场应具备良好的通风、照明和操作空间的条件；赛场需留有安全通道，必须配备灭火设备。

3.赛场须配备相应的医疗人员和急救人员，并备有相应急救设施。

（四）项目特别规定

项目特别规定用于提供该赛项所特定的一些细则。项目特别规定包括但不限于：个人 IT 设备、数据存储设备、因特网接入、程序和工作流程、文档管理和发放，项目特别规定列表如下：

项目/任务	项目特别规定
使用技术/个人照相机	裁判员——任何情况下，不得携带个人照相机进入竞赛场地中的选手工位，除非由裁判长或裁判长助理批准 选手——不得将照相机带入场地
使用技术/移动设备	裁判员——任何情况下，不得携带任何电子设备进入竞赛场地中的选手工位，除非由裁判长批准。 选手——电子设备（包括移动电话）必须存放在选手背包（关机或静音）并放于储物柜中。任何情况下，不得携带任何电子设备进入竞赛场地中的选手工位，除非由裁判长或裁判长助理批准
资源文件/笔记	选手——任何情况下，不得携带笔记进入竞赛场地，竞赛期间在选手竞赛场地工位中记录的必须全程都留在选手桌上，不得将任何笔记带出竞赛场地
设备故障	选手——如果出现设备故障，选手必须立即举手通知裁判员，裁判员应将选手因故障不能操作的时间记录在案；因设备故障导致的时间损失，将在模块的规定时间之外给予补时；因设备故障前未能存盘导致的时间损失将不予补时。